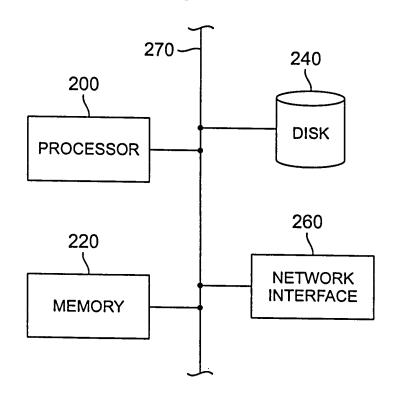


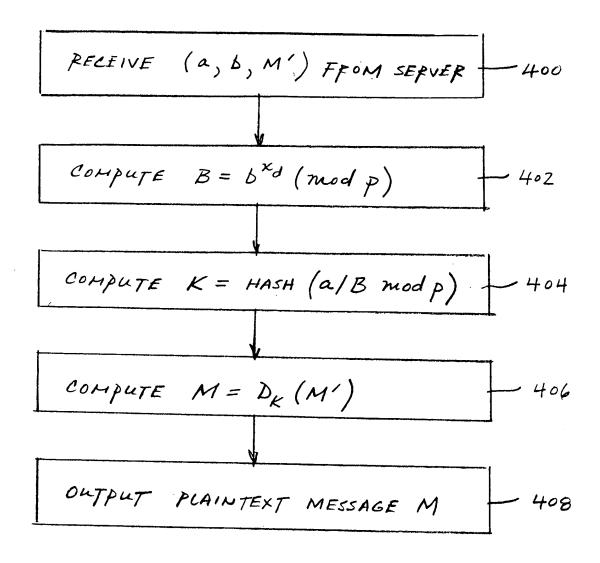
F16.1



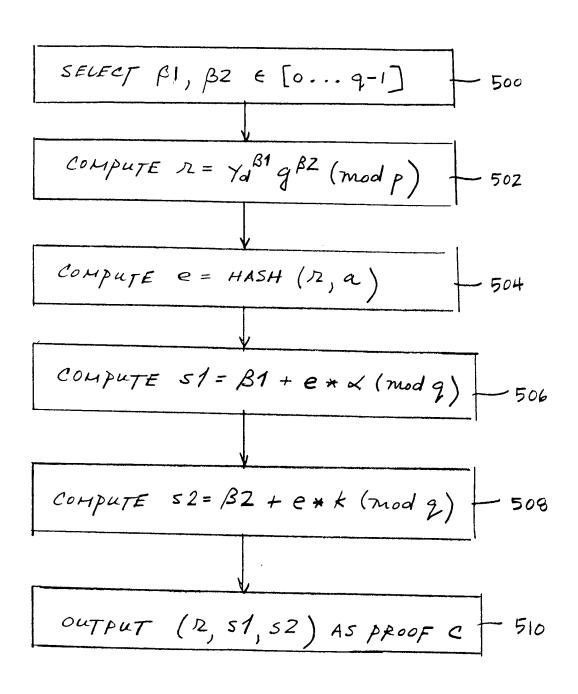
F16, 2

GENERATE A MESSAGE M TO BE 300 FNCRYPTED PICK A PANDOM ELEMENT K & [0...9-1] COMPUTE A SYMMETRIC KEY K = HASH (gk mod p) SUCH THAT K ISA 304 VALID ENCRYPTION KEY FOR A GIVEN ENCRYPTION TECHNIQUE COMPUTE A QUINTUPLE (a, b, M', C, Cd) 306 WHERE a = Yagk, b = gd, M' = EK(M), (is a proof of Knowledge of (d, k), AND Cd is A CERTIFICATE ON PUBLIC KEY Yd SEND (a, b, M', C, Cd) THROUGH THE 308 NETWORK WITH INFORMATION IDENTIFYING SENDER AND RECIPIENT

716,3



F16. 4



F16, 5

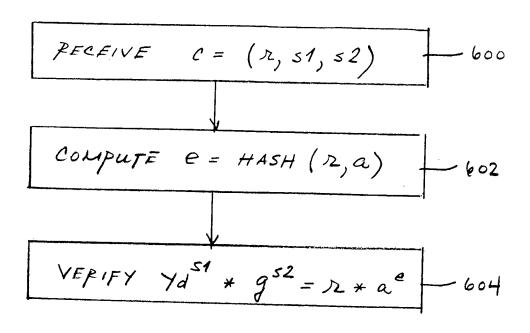


FIG. 6